JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
OFFICE OF FINANCIAL AND INSURANCE SERVICES
DEPARTMENT OF LABOR & ECONOMIC GROWTH
ROBERT W. SWANSON, DIRECTOR

LINDA A. WATTERS
COMMISSIONER

DATE: October 16, 2006

LETTER NO.: 2006-CU-07

TO: The Board of Directors and Management of Michigan-Chartered Credit Unions

SUBJECT: Information Technology (IT) Examinations

This letter supersedes the Office of Financial and Insurance Services' (OFIS) Credit Union Letter No: 2004-CU-01, 'Information Technology Examinations'.

Purpose of this Letter

The purpose of this letter is to clarify the IT examination process, compliance expectations, examination guidance, and incorporate changes in the Uniform Rating System for Information Technology.

IT Examination Background

Regulatory supervision of IT operations is necessary with the integration of increasingly complex technologies and the resulting risk exposure. While OFIS has performed credit union IT examinations since the early 1970s, the scope and frequency of these examinations varied. In 2004, OFIS created a standardized IT examination program.

IT Examination Program

Examination Process:

The IT Examination Program is a risk based program. As such, the frequency of IT examinations is affected by prior examination findings, institutional complexity, management changes, system changes, and other factors.

An IT examination evaluates a credit union's IT environment and management planning through a top-down approach. The examination evaluates how well management understands, administers, and secures the IT environment. During this process, examiners review IT related policies and procedures, audit reports, disaster recovery planning, patch management, systems' logical and physical security, and other related areas. Findings and recommendations are formalized and mailed to the board chairperson in a stand alone IT Examination Report. The Board of Directors is required to formally respond to each finding and recommendation in the report.

Ratings:
Each IT examination results in assigned component and composite ratings. The four component areas are 'Audit', 'Management', 'Development and Acquisition', and 'Support and Delivery' which are discussed in detail in the Examination Scope section of this letter. IT examination ratings range from '1' to '5'; a '1' indicates exemplary performance, while a '5' indicates serious problems requiring regulatory intervention.

The IT Examination composite rating is not necessarily an average of the four component ratings. Depending on the severity of the findings, a single component rating may significantly influence the composite rating.

The IT Examination composite rating is considered when determining a credit union's overall CAMEL rating. Under the CAMEL rating system, this is typically manifested in the 'M' or 'Management' rating. While a 3 or lower IT composite rating does not necessarily result in a '3' or lower Management rating, it is a factor in the rating and can indicate management weaknesses. Examiners will continue to be responsible for assigning ratings in the CAMEL system under the Safety and Soundness Examination process. If IT related weaknesses negatively impact the Safety and Soundness Management or Composite rating, disclosure of the weakness and its perceived significance will be included within the report of examination.

Examination Scope:
IT examinations encompass four main areas:

<u>Audit</u> - Examiners review the most recent external or internal audit report(s), as well as reports on vulnerability assessments. Examiners also review IT audit scope and frequency as it relates to the credit union's information security risk assessment.
<u>Management</u> - Examiners review IT policies and procedures, strategic planning, ability and willingness to correct previous audit and examination deficiencies, and compliance with rules and regulations.
<u>Development and Acquisition</u> - Examiners review policies and procedures regarding the acquisition of significant new hardware and software, vendor remote access, contracts, and patch management processes.
<u>Support and Delivery</u> - Examiners review internal controls and segregation of duties, logical and physical security considerations, ACH/wire transfer operations, as well as disaster recovery planning and testing.

Compliance Expectations:
Each Board of Directors and management team are expected to correct IT examination deficiencies within an appropriate time frame. Failure to correct the identified weaknesses may result in financial and/or reputation loss due to disclosure of confidential member information. Safety and Soundness examiners will follow-up on management's corrective efforts, which may impact the overall Management rating. OFIS expects each Board of Directors and management team to correct weaknesses and mitigate IT risks to the greatest extent possible.

Examination Guidance:

OFIS' IT Examination program follows the guidance established by the Federal Financial Institutions Examination Council (FFIEC)[1], which uses resources from each federal depository/insurance regulatory agency. The IT examination program also incorporates many standards established by non-regulatory resources, such as Information Systems Audit and Control Association (ISACA), National Institution of Standards and Technology (NIST), and Control Objectives for Information and related Technology (COBIT).

To fully explore the IT Examination process , management should consult the FFIEC IT Handbook InfoBase available via the FFIEC website (www.ffiec.gov). The InfoBase includes IT Handbooks on areas such as business continuity, Fedline, e-banking, and a glossary of IT terminology. To obtain a hard copy of the IT Booklets, management must contact the National Credit Union Administration (NCUA) but printable versions are available on the FFIEC website. Management can also consult the following websites for more information:

Information Systems Audit and Control Association (www.isaca.org).
National Institute of Standards and Technology (www.nist.gov).
IT Governance Institute (www.itgi.org).
International Organization for Standards (www.iso.org).

Conclusion

Credit unions increasingly use information systems and electronic technology to both lower costs and provide increased value to the membership. With any new technology, management must take a proactive approach to identify, measure monitor and control risk exposure. The IT examination process recognizes the significance and pervasiveness of this area and the need for targeted review by qualified individuals. OFIS also hopes the process will help management identify and mitigate risk exposure, as well as provide guidance on regulatory and industry-best practices.

Questions regarding this letter and IT examination issues may be directed to Brent Moeggenborg at 517-373-6930.

Sincerely,

Roger W. Little, Deputy Commissioner
Credit Union Division

[1] The FFIEC is comprised of the five financial institution regulatory agencies: Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), Office of Comptroller and Currency (OCC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA).